FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1669686-000

Total Deleted Page(s) = 19
Page 11 ~ Duplicate;
Page 12 ~ Duplicate;
Page 13 ~ Duplicate;
Page 16 ~ Duplicate;
Page 17 ~ Duplicate;
Page 20 ~ Duplicate;
Page 21 ~ Duplicate;
Page 24 ~ Duplicate;
Page 25 ~ Duplicate;
Page 28 ~ Duplicate;
Page 29 ~ Duplicate;
Page 34 ~ Duplicate;
Page 35 ~ Duplicate;
Page 36 ~ Duplicate;
Page 37 ~ Duplicate;
Page 40 ~ Duplicate;
Page 41 ~ Duplicate;
Page 46 ~ Duplicate;
Page 50 ~ b6; b7C; b7E;

XXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXX

[redacted] b7E

 b6 b7C

AIPAC's WWW site receives about 2,000 users per day. The AIPAC site allows visitors to input information, i.e. credit card numbers, name, address, and email addresses, if desired. To better ensure the information a visitor inputs onto AIPAC's WWW site is secure from unauthorized access, [redacted] b6 b7C b7E

[redacted]

Attached to this communication are the Serv-u FTP log files for [redacted] Also enclosed in a FD-340 envelope is a printout of daily visitor statistics for the AIPAC WWW site. b6 b7C b7E

Also present at the interview was Special Agent [redacted]

 b7E

Fusion e-commerce engine and stored in an Access database. The information is then accessed by AIPAC personnel who regularly FTP to the web server both to retrieve the databased information and to upload changes to their site. The personal information can contain, depending on the business being conducted by the visitor, the visitor's name, address, phone number(s), and credit card information. The web page installed by the UNSUB(S) on AIPAC's site contained links to this information, making it available to anyone accessing AIPAC's altered website.

Shortly after AIPAC personnel discovered that their site had been illegally accessed and altered, the site was taken off-line. As of 11/02/2000, despite an aggressive notification campaign aimed at their compromised membership, AIPAC had received no complaints of fraudulent credit card usage.

In light of the foregoing information, it is recommended this case be O&A'd to the writer. Additionally, it is requested SA [redacted] be assigned to this matter as co-case agent. b6 b7C

♦♦

Title and Character of Case:

PAKISTAN HACKERZ CLUB
AMERICAN ISRAEL PUBLIC AFFAIRS COMMITTEE

Date Property Acquired: 11/06/2000

Source from which Property Acquired: WEBFIRST [redacted] b6 b7C

Anticipated Disposition: [redacted]

Acquired By: [redacted]

Case Agent: [redacted]

Description of Property: Date Entered

1B 1

100 MB ZIP CARTRIDGE CONTAINING FTP LOGS FOR WEBFIRST'S RAVEN SERVER ON 11/6/2000

Barcode: E01823347 Location: ECR/MMOC CAB 11/28/2000

FILE

Case Number: [redacted] b7E
Owning Office: BALTIMORE

1B1

Title and Character of Case:

PAKISTAN HACKERZ CLUB
AMERICAN ISRAEL PUBLIC AFFAIRS COMMITTEE

Date Property Acquired: 11/09/2000

Source from which Property Acquired: WEBFIRST [redacted] b6 b7C

Anticipated Disposition:

Acquired By: [redacted]

Case Agent: [redacted]

Description of Property: Date Entered

1B 2

1GB JAZ CARTRIDGE CONTAINING THE FOLLOWING LOGS FROM WEBFIRST'S RAVEN SERVER AS OF 11/9/2000:
COLD FUSION LOGS
COLD FUSION MAIL LOGS
II'S LOGS FOR ALPAC'S WWW SITE
NT SERVER LOGS
WWW LOGS FOR THE FASHIONSITE ON RAVEN

Barcode: E01823348 Location: ECR/MMOC CAB 11/28/2000

FILE

Case Number: [redacted] b7E
Owning Office: BALTIMORE

1B 2

Title and Character of Case:

PAKISTAN HACKERZ CLUB
AMERICAN ISRAEL PUBLIC AFFAIRS COMMITTEE

Date Property Acquired: Source from which Property Acquired:

02/26/2001 [redacted](WEBFIRST)

b6
b7C

Anticipated Disposition: Acquired By: Case Agent:

[redacted] [redacted]

Description of Property: Date Entered

1B 3

100MB ZIP CARTRIDGE WITH RAVEN FTP LOG FILES FOR 08/03/2000-11/08/2000

Barcode: E01823450 Location: ECR/MMOC CAB 02/26/2001

FILE

Case Number: [redacted]

b7E

Owning Office: BALTIMORE

1B3

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 11/10/2000

On 11/8/2000, [redacted] faxed information pertaining to the fraudulent use of VISA card [redacted] owned by [redacted] and MasterCard [redacted] owned by [redacted] to SA [redacted] The fax is attached to this communication for inclusion in the file. b6 b7C

[redacted] b7E

SEARCHED
ENTERED
UPDATED
NO ACTION

[redacted] b6 b7C

Investigation on 11/8/2000 at Calverton, Maryland

File # [redacted] Date dictated 11/10/2000 b7E

by SA [redacted]

12/12/00

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

343 [redacted] 13,302

AIPAC

AIPAC

Phone: 202-639-5200
FAX: [redacted]
em[redacted]

b6
b7C

Facsimile

To: [redacted]
@Fax: 301-686-4544
From: [redacted]
Date: Wednesday, November 8, 2000 @ 4:30PM
Re: Credit card fraud
Pages: 2, including this

b6
b7C

[redacted]

We have received reports from people with unauthorized charges on their credit cards. Their information is on the following page.

Thanks

[redacted]

b6
b7C

- business phone number [redacted]
- VISA [redacted]
- charge of $485.03 to a video chat site (friends wpi)
- he received notice from his credit card company Thursday afternoon for suspicious charges to his VISA
- when he called the video-chat company they confirmed the charge and said they thought the person using his card was talking with someone in the Philippines with the name [redacted] (not sure about the spelling in address)
-

[redacted]

b6
b7C

- [redacted]
- Mastercard [redacted]
- Reported three internet charges
- 1.) $1
- 2.) $79.95 at paycom
- 3.) ?

TOTAL P.02

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 11/14/2000

On 11/9/2000, [redacted] faxed information pertaining to the fraudulent use of American Express card [redacted] owned by [redacted] to SA [redacted] The fax is attached to this communication for inclusion in the file. b6 b7C

(1)

[redacted] b7E

SEARCHED
ENTERED
UPDATED
NO

[redacted] b6 b7C

Investigation on 11/9/2000 at Calverton, Maryland

File # [redacted] Date dictated 11/14/2000 b7E

by SA [redacted]

12/12/00

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

[redacted] 12.302

Memorandum

To: [redacted] b6 b7C

From: [redacted]

Date: 11/9/2000

Re: Credit card fraud

There has been another reporting of credit card fraud. The man's name is [redacted] and his phone number is [redacted] The credit card was an American Express [redacted] b6 b7C

[redacted] received a call from a man in Cleveland, Ohio who owns a company called Drifterbags.com. The owner told [redacted] that a backpack being shipped to Indonesia had been charged on [redacted] AMEX card, which [redacted] did not order. The owner said he had been receiving a bunch of orders that people where people were using fraudulent credit cards so he was checking out all charges now. They did not get the owner's name or phone number.

Also, I sent you another report of credit card fraud that happened today for a [redacted] His phone number is [redacted]

[redacted]

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 11/14/2000

On 11/10/2000, [redacted] faxed information pertaining to the fraudulent use of MasterCard [redacted] owned by [redacted] to SA [redacted] The fax is attached to this communication for inclusion in the file. b6 b7C

[redacted] b7E

SEARCHED [redacted]
ENTERED [redacted]
UPDATED [redacted]
NO ACTION [redacted]

[redacted] b6 b7C

Investigation on 11/10/2000 at Calverton, Maryland

File # [redacted] Date dictated 11/14/2000 b7E

by SA [redacted]

[redacted] 11/14/00

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

[redacted] FD-302

Memorandum

To: [redacted] b6 b7C

From: [redacted]

Date: 11/10/2000

Re: Credit Card Fraud

We have another report of credit card fraud from one of AIPAC's members. The man's name is [redacted] His credit card was a Mastercard, [redacted] b6 b7C

[redacted] has already cancelled his credit card but said there were thousands of dollars worth of fraudulent charges made on it. He could only give me the name of one place it was used for $250. The name of the place is PAYPAL and [redacted] has already contacted them to try and get more information. [redacted] spoke with [redacted] The company is located in Palo Alto, California and their phone number is [redacted]

In addition, [redacted] told me he would like to press charges against the people who committed this credit card fraud. I gave him your phone number.

Please let me know if you need more information.

Thank you.

[redacted]

[redacted]

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 11/15/2000

On 11/14/2000, [redacted] faxed information pertaining to the fraudulent use of VISA card [redacted] owned by [redacted] and VISA card [redacted] owned by [redacted] to SA [redacted] The fax is attached to this communication for inclusion in the file. b6 b7C

[redacted] b7E

SEARCHED
ENTERED
UPDATED
NO ACTION

[redacted] b6 b7C

Investigation on 11/14/2000 at Calverton, Maryland

File # [redacted] Date dictated 11/15/2000 b7E

by SA [redacted] 11/12/00

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

Memorandum

To: [redacted] b6 b7C

From: [redacted]

Date: 11/14/2000

Re: More Credit card fraud

There has been another two more reports of credit card fraud. The first man's name [redacted] b6 b7C
His credit card is a Visa, [redacted]

[redacted] had a couple $1000 charged to his credit card. There were three charges and he only knew the specifics of one. The name of the company is BlackOak Computers in Southern California and they contacted [redacted] because the charge was for $1250/month. [redacted] spoke with a male [redacted] at BlackOak Computers, whose phone number is [redacted] The other part of this is whoever charged this on [redacted] credit card was having the "product" sent to [redacted] residence. I don't really know what that means.

One last piece on [redacted] credit card fraud is he gave me the name and number of the person he spoke with at the Visa Fraud Unit. He spoke with [redacted] b6 b7C

The second guy who had credit card fraud is [redacted] and his credit card a Visa, [redacted] is supposed to e-mail more information about the specifics of the charges and I will forward that on to you. [redacted] phone number is [redacted]

I will send you another fax tomorrow.

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 11/15/2000

On 11/14/2000, [redacted] faxed information pertaining to the fraudulent use of VISA card [redacted] owned by [redacted] to SA [redacted] The fax is attached to this communication for inclusion in the file. b6 b7C

(1)

[redacted] b7E

SEARCHED
ENTERED
UPDATED
NO ACTION

[redacted] b6 b7C

Investigation on 11/14/2000 at Calverton, Maryland

File # [redacted] Date dictated 11/15/2000 b7E

by SA [redacted]

12/12/00

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

√343 [redacted] 09.302

Memorandum

To: [redacted] b6 b7C

From: [redacted]

Date: 11/14/2000

Re: Credit card fraud

There has been another reporting of credit card fraud. The man's name is [redacted] and his phone number is [redacted] The credit card was a Visa [redacted] phone number is [redacted] b6 b7C

I spoke with [redacted] yester day and he said he had over $3000 worth of credit card fraud. The fraudulent charges were made in Sept. and Oct., so [redacted] thinks the hackers may have had access to the info before they published it. On September 22,23 and 26 there were charges made to AIRTRAN, leaving from Atlanta. And on October 3, 10 and 20 there were charges made to a store called Mr. Everything in Atlanta.

There were two other people who had fraudulent charges on their cards who I have not gotten in touch with yet. I will send you their info when I do.

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 11/16/2000

On 11/15/2000, [redacted] faxed information pertaining to the fraudulent use of a credit card owned by [redacted] b6 b7C
[redacted] to SA [redacted] Included in this fax is a printout of an email received by [redacted] The fax is attached to this communication for inclusion in the file.

[redacted] b7E

SEARCHED
ENTERED
UPDATED

[redacted] b6 b7C

Investigation on 11/15/2000 at Calverton, Maryland

File # [redacted] Date dictated 11/16/2000 b7E

by SA [redacted]

[redacted] 12/12/00

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

~~347~~ [redacted] 08.302

[Click here and type address]

facsimile transmittal

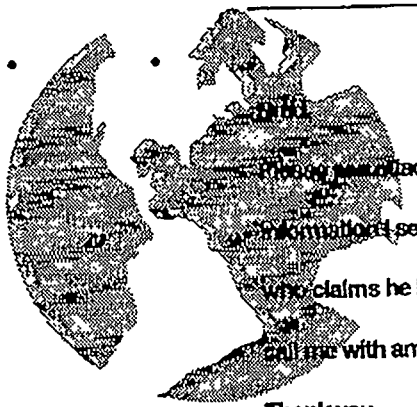
To: [redacted] Fax: 301-586-4488 b6 b7C

From: [redacted] Date: 11/15/2000

Re: Additional info on fraud Pages: 3

CC: [Click here and type name]

☑ Urgent ☐ For Review ☐ Please Comment ☐ Please Reply ☐ Please Recycle



Please see attached document. It gives addition information about [redacted] whose b6 b7C information I sent to you yesterday, credit card fraud. Also, I received this e-mail from a [redacted] who claims he knows of some Muslim hackers that have been breaking into Israeli web sites. Please call me with any questions at [redacted]

Thank you

[redacted]

CONFIDENTIAL

b6
b7C

[redacted] the charges were as follows:

11/10	bargain property networks	9.95
11/10	bargain property networks	88.90

they said both charges were from [redacted] of Pine Bluff, Arkansas.

bargain property networks customer service can be reached at 800-333-1915.

thanks, [redacted]

(FBI)

b6
b7C

(3)

Hi, as you know, lots of Israeli websites have been Hacked by Pro Muslim Groups. I know the Muslims behing the hacking. Can you contact the FBI and tell them this. An Arab group calling itself UNITY (www.unity-news.org) has taken a leading role in the war, which it says is designed to sap the resources of Israel and thereby weaken its military strength. "The more money they lose in fixing and strengthening their systems means less money to buy bullets and rockets for use against our children," UNITY said in an e-mail release sent to Arab organizations and media outlets early this month, instructing its supporter to visit two "counter attack" links. "Every dollar they lose means one less bullet for the Zionist soldiers' ammunition. " the e-mail said. The Islamic Gateway World Wide Media Network (www.ummah.net) has also been implicated in several attacks involving "denial of service" assaults similar to those that paralyzed Yahoo! and eBay were paralyzed earlier this year. UNITY has begun listing various Israeli e-commerce sites on its hit list in an effort to strike at the country's leading high tech industry. One Israeli Internet company, Webstyle Internet Solutions (www.web-style.com), has already announced plans to transfer all of its local hosting to the U.S. to avoid attacks. Netvision, a leading Israeli ISP which houses several official government sites, has been struggling to keep its servers running smoothly. "All Israeli ISPs have been overloaded with data, we are just the only ones to admit it," says [redacted] b6
[redacted] "If this war continues it will steal b7C
resources from us and hurt customers."2

[redacted]

Do You Yahoo!?
Yahoo! Calendar - Get organized for the holidays!
http://calendar.yahoo.com/

(FBI)

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 11/16/2000

On 11/15/2000, [redacted] faxed information pertaining to the fraudulent use of MasterCard number [redacted] owned by [redacted] and American Express card [redacted] owned by [redacted] to SA [redacted] The fax is attached to this communication for inclusion in the file. b6 b7C

(1)

[redacted] b7E

SEARCHED ____
ENTERED ____
UPDATED ____
NO ACTION ____

[redacted] b6 b7C

Investigation on 11/15/2000 at Calverton, Maryland

File # [redacted] Date dictated 11/16/2000 b7E

by SA [redacted]

12/12/00 [redacted]

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

[redacted] 07.302

Memorandum

To: [redacted]

From: [redacted]

Date: 11/15/2000

Re: More Credit card fraud

b6
b7C

There have been two more reports of credit card fraud. The first man's name is [redacted] and his phone number is [redacted] His credit card is a Mastercard, [redacted] had one fraudulent charge on his credit card for $394 and it came from Austin, TX.

b6
b7C

The second guy who had credit card fraud is [redacted] and his credit card is an AMEX, [redacted] had a couple $1,000 charged on his credit card. One charge was for a computer for $2,000. All of the items charged were supposed to be sent to Pakistan. Also, there was an e-mail address on the orders [redacted] phone number at work is [redacted] and at home is [redacted]

I will send you another fax tomorrow.

FD-542 (Rev. 11-02-1999)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 12/19/2000

To: Baltimore

From: Baltimore
SQ 23
Contact: SA [redacted] 301-586-4516 b6 b7C

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (Pending) b7E

Title: UNSUB(S), aka [redacted]
PAKISTAN HACKERZ CLUB;
AMERICAN ISRAEL PUBLIC
AFFAIRS COMMITTEE - Victim;
INTRUSION - INFO SYSTEMS

Synopsis: To report investigative accomplishments associated with the captioned matter.

Details: Since the captioned matter was O&A'd to the writer on 11/03/2000, the following investigative accomplishments have been achieved:

[redacted] b6 b7C

[redacted] b7E

SEARCHED
ENTERED
UPDATED
NO ACTION

[redacted] b6 b7C

[redacted] 2.542

To: Baltimore Fro Baltimore
Re: [redacted] 12/19/2000 b7E

Accomplishment Information:

Number: 1
Type: [redacted] COMPROMISED SITE IDENTIFIED AND NOTIFIED b6 b7C b7E
ITU:
Claimed By:
SSN: [redacted]
Name:
Squad: 23

Number: 1
Type: [redacted] FOREIGN SOURCE IP ADDRESS IDENTIFIED
ITU: COMPUTER ASSISTANCE
ITU: [redacted]
Claimed By:
SSN: [redacted]
Name:
Squad: 23

Number: 1
Type: [redacted] INFORMANT/ASSET DEVELOPED b6 b7C b7E
ITU:
Claimed By:
SSN: [redacted]
Name:
Squad: 23

Number: 1
Type: [redacted] SUBJECT IDENTIFIED
ITU:
Claimed By:
SSN: [redacted]
Name:
Squad: 23

Number: 4
Type: [redacted] VICTIM CONTACTED/INTERVIEWED
ITU:
Claimed By:
SSN: [redacted]
Name:
Squad: 23

To: Baltimore Fro[redacted] Baltimore
Re: [redacted] 12/19/2000

b7E

LEAD(s):

Set Lead 1: (Adm)

BALTIMORE

AT CALVERTON

Read and clear.

♦♦

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 12/21/2000

Source, who is not in a position to testify, provided the following information:

[redacted]

b6
b7C
b7D

[redacted]

b7E

b6
b7C
b7D
b7E

I:\ORAPS\14[redacted] 35[redacted] 302 [redacted] 12/21/2000

Investigation on 12/19/2000 at Calverton, Maryland (telephonically)

File # [redacted] Date dictated 12/21/2000

by SA [redacted]

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

Automated Serial Permanent Charge-Out
FD-5a (1-5-94)

Date: 01/17/01 Time: 10:37

Case ID: [redacted] b7E

Description of Document:

Type : FD302
Date : 01/03/01
To : BALTIMORE
From : SAN FRANCISCO
Topic: [redacted] b6 b7C

Reason for Permanent Charge-Out:

serialized into wrong file

Employee: [redacted]

[redacted] b7E b6 b7C

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 11/07/2000

[redacted] b6 b7C

[redacted] located at 13500 Piccard Avenue, Suite 101, Bethesda, Maryland, work telephone number [redacted] was interviewed at [redacted] After being advised of the identities of the interviewing agents and the nature of the interview, the following information was provided:

On 11/01/2000, [redacted] was told by American Israel Public Affairs Committee (AIPAC) employees that AIPAC's WWW site was defaced and information contained in AIPAC's Access database had been compromised. The defacement contained anti-semitic language and wording crediting the "Pakistan Hackerz Club" (PHC) for the defacement. Investigation by [redacted] revealed that [redacted] b6 b7C b7E

[redacted]

AIPAC, a WebFirst customer for the past two years, is currently one of 50 WebFirst customers whose WWW pages are hosted [redacted] b7E

[redacted] b6 b7C b7E

Investigation on 11/06/2000 at Bethesda, Maryland

File # [redacted] Date dictated 11/07/2000

by SA [redacted]

SEARCHED
ENTERED
UPDATED
NO ACTION

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

312 [redacted] 01.302

(Rev. 10-01-1999)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 11/03/2000

To: Baltimore

From: Baltimore
SQ 14/MMOC
Contact: SA [redacted] 301-586-4516 b6 b7C

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (Pending) b7E

Title: UNSUB(S), aka [redacted]
PAKISTAN HACKERZ CLUB;
AMERICAN ISRAEL PUBLIC
AFFAIRS COMMITTEE - Victim;
INTRUSION - INFO SYSTEMS

Synopsis: To recommend the captioned matter be opened for investigation.

Details: On 11/02/2000, the writer spoke telephonically with [redacted] b6 b7C They advised that their website, aliased as both aipac.com and aipac.org, had been illegally accessed and subsequently defaced. Additionally, two Microsoft Access databases containing e-mail addresses and personal information on AIPAC members and associates had been compromised on the Internet.

[redacted] described AIPAC as an organization which lobbies Congress on bills pertaining to Israel. AIPAC's website is hosted by WebFirst, Inc. of Bethesda, Maryland, on a web server which is also located in Bethesda. Sometime on 11/01/2000, UNSUB(S) identified as [redacted] of the PAKISTAN HACKERZ CLUB illegally gained access to the aforementioned web server and replaced AIPAC's opening web page with a page containing anti-Israeli propaganda, links to other anti-Israeli and pro-Palestinian websites, and links to the e-mail addresses and personal information stolen from the databases.

[redacted] b6 b7C

Visitors to the AIPAC website are provided with an opportunity to enter personal information for a variety of reasons, including joining AIPAC or registering for an AIPAC sponsored event. The information is entered through a Cold b6 b7C b7E

311 [redacted] 01, EC
[redacted]
ENTERED
UPDATED
NO ACTION

Of A Ney [redacted]
Case
Assign to
[redacted]